NETSPI™

5 Strategies for Log4j Vulnerability Identification

800 Washington Ave. N.
Suite 670
Minneapolis, MN 55401

E : info@netspi.com
W : www.netspi.com
P : 612.465.8880

NETSPI™

Let’s face it, no organization has perfect asset management practices. For those that do, congratulations, you likely have a better handle on your Log4j remediation strategy. For the rest of us, understanding Log4j usage in your environment should be at top of your to-do list.

When you consider this issue is represented across thousands of products, many of which are produced by major software providers, it's unlikely that anyone is not impacted to some degree. We believe that organizations should assume they are impacted until they prove otherwise.

For organizations with managed (owned and operated by your organization) and unmanaged (black box, connected to the network) environments, here are five key strategies to identify vulnerable Log4j instances.

Table of **Contents**

03 >> **Strategy 1**
Full Port Vulnerability Scanning

04 >> **Strategy 2**
Log4j File Scanning

04 >> **Strategy 3**
Collaborate with Your Development Teams

05 >> **Strategy 4**
Vendor Risk Management

06 >> **Strategy 5**
Team up with NetSPI

Strategy 1: Full Port Vulnerability Scanning

- Perform full port vulnerability scanning with service fingerprinting enabled. Use a scanning tool like nmap to allow you to identify commonly abused protocols like HTTP and Remote Method Invocation (RMI).
- Using the live host and port list, conduct server layer vulnerability scanning using tools like Nessus or Nexpose. They can identify vulnerable Log4j instances by injecting into the top HTTP Header injection points. This approach, which includes full port scanning, should take minimal effort if executed from a single location. *Note: Nessus and Nexpose can also be configured to perform full port scanning and fingerprinting.*
- Vulnerability scanning tools can also identify RMI services that are hosted by Java applications. When possible, fingerprint that and contact your RMI services vendor to determine if they use Log4j. If the product is open source, simply review the code online.
- Using the Nessus or Nmap output, configure EyeWitness or another screen scraping tool such as WitnessMe or Aquatone, to perform screen scraping of available websites. This will provide you with a catalog of websites to review. Using the information it provides, identify web applications that may need to be targeted for more comprehensive testing.
- Once you've identified a list of web applications, Burp Suite Pro can be used with the Log4Shell Scanner plugin. It will identify vulnerable Log4j instances by injecting exploitable strings that will initiate a callback to the user into all the dynamic elements of the web application it can map.

Safety Tips for Unauthenticated Full Port Scans

- Consider starting with the most common web ports first: 80,81, 82,443,5432,2902,5800,5900,5700,8000, 8300,8080,8500,8501,8433,8888,8900,51010,9090,9100,9000, 10000.
- Scanning tools can be throttled so they don't overwhelm the state tables, CPU, or other network devices (e.g. scanners, firewalls).
- To avoid scanning through firewalls, in some cases you can deploy a scan to the target subnet. That way traffic may flow through the switch infrastructure, but not hit the firewall. *Note: this is highly dependent on configuration.*

Strategy 2: Log4j File Scanning

- Log4j is an open source project. As such, you can download it and create an inventory of all the files that are used by the package. Ideally targeting files that are unique to Log4j.
- It may be possible to use this list to leverage existing EDR, File Integrity Monitoring (FIM), and configuration management tools that already exist in the environment to identify vulnerable instances of Log4J. *Note: In theory, the same list could be used as a dictionary against web servers.*

Strategy 3: Collaborate with Your Development Teams

- Go to your asset management portal and get a list of all the internally developed apps and application owners.
- Send out a message asking application owners to tell you if their solution uses Log4j or not.
- For those that do, work with them to apply the required patches.

Strategy 4:
Vendor Risk Management

Reach out to vendors to determine if vulnerable Apache Log4j versions are being used for applications that were not developed by your company that have already been deployed to the environment. Key questions to ask, include:

1. Does [organization] leverage Log4j or related Apache components?
2. Is your company vulnerable to the Log4j vulnerabilities?
3. Have you tested your networks to ensure unauthorized parties have not gained access to your environment?
4. Have you experienced any unauthorized activity or malicious behavior in your environment?
5. Have you updated to the latest non-vulnerable version of Log4j?
6. Have you taken the steps to implement the patches released by Apache?
7. Will Log4j remediation efforts impact service?
8. Do you have third parties that process client data? Are they vulnerable?
9. Have any of your third-party/fourth-party partners reported service disruption or impairment?

Strategy 5: Team up with NetSPI

Don't have the time or resources to complete the above? Want third-party validation of your Log4j remediation efforts? Our testing team developed a comprehensive Log4j testing methodology that leverages our penetration testing and vulnerability management technologies, Resolve and Scan Monster. Here is an overview of the base services available:

- Testing of up to 500 external total IP addresses
- Unauthenticated scanning for common injection points in identified web applications used to abuse vulnerable Log4j instances
- Testing may include exploitation of identified vulnerable Log4j instances
- Testing will be conducted from NetSPI facilities
- Testing will be done in a production environment
- A testing schedule will be coordinated between NetSPI project managers and client stakeholders
- Both automated and manual testing (scanning) will not be restricted to specific times of day and may occur 24x7
- Additional services available: Remediation testing, attestation letter, scoping of larger assessments

How it Works

- We use automated service discovery from assets provided. Then, we feed that information into our Log4j vulnerability scanning technology, Scan Monster.
- It crawls through services, testing parameters, headers, and cookies using verified exploitable strings that will trigger callbacks from vulnerable Log4j implementations.
- Many existing scanners out there are just testing headers in HTTP requests, poorly sometimes. We are crawling and testing every part of a discovered service's attack surface.
- We have tested our scanning workflow against vulnerable services and have validated its efficacy in multiple instances.

NETSPI™

Whatever the approach you take, NetSPI's experts are here to help. Ready to get started?

Want more Log4j discovery and remediation advice?

Contact sales@netspi.com.

ABOUT NETSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest healthcare companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve™ platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.